IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Previously Presented): An encryption processing apparatus configured to perform a data encryption process, said encryption processing apparatus comprising:

a processor configured to provide:

a control section configured to set a mixed encryption processing sequence by dividing an original encryption processing sequence into a plurality of groups, each group being composed of a plurality of encryption processing units, each encryption processing unit being a defined process, each group being a separate and independent encryption process for encrypting an input data, where a first input data to be encrypted for a first group of the groups is different relative to a second input data to be encrypted for a second group of the groups, and the first input data to be encrypted for the first group is generated independently relative to the second input data to be encrypted for the second group, said control section mixing processing sequences of encryption processing units of the plurality of groups with each other by executing performance of at least one encryption processing unit from the first group at a time between executing performance of encryption processing units from the second group and under a condition in which a processing sequence of the encryption processing units within each of the plurality of groups is fixed;

an encryption processing section configured to perform an encryption process in accordance with the mixed encryption processing sequence set by said control section; and

a transmitting unit configured to transmit each of encrypted output data generated independently by the first group and the second group to an external device.

Claim 2 (Previously Presented): The encryption processing apparatus according to Claim 1, wherein each group includes a triple-DES encryption process and said control

section is configured to set a dummy single-DES process as a dummy encryption process that is unnecessary for an encryption processing sequence in at least one of said groups, and set the number of dummy single-DES processes to be a multiple of 3, and wherein said control section is configured to set a dummy encryption processing unit that performs the dummy encryption process in at least one of the groups, and set one mixed encryption processing sequence by mixing the encryption processing units of a plurality of groups containing the dummy encryption processing unit.

Claim 3 (Previously Presented): The encryption processing apparatus according to Claim 1, wherein said control section is configured to determine a group of sequences, which can be performed independently of each other, within the original encryption processing sequence to be divided in a process of division into the plurality of groups, and perform a process for setting a group of divisions in which each of the sequences in the group of sequences can be performed independently as a unit.

Claim 4 (Previously Presented): The encryption processing apparatus according to Claim 1, wherein said encryption processing unit is a single-DES encryption process, and

wherein said control section is configured to set the mixed encryption processing sequence by dividing the original encryption processing sequence containing one or more single-DES encryption processes into a plurality of groups composed of one or more single-DES encryption processes and by mixing the single-DES encryption processing units contained in each group by mutual replacement of the single-DES encryption processing units of each set group under the condition in which the processing sequence within each set group is fixed.

Claim 5 (Previously Presented): The encryption processing apparatus according to Claim 1, wherein said control section is configured to perform a process for dividing the encryption processing sequence into a plurality of groups composed of one or more encryption processing units by using a single-DES encryption process which forms a triple-DES encryption process as an encryption processing unit.

Claim 6 (Previously Presented): The encryption processing apparatus according to Claim 1, wherein the original encryption processing sequence to be mixed is an encryption processing sequence including a random-number generation process, and

said control section is configured to form a random-number generation process as a process including a conversion process by three single-DES processes, and sets the three single-DES processes as a random-number generation process in one of the groups of divisions.

Claim 7 (Canceled).

Claim 8 (Previously Presented): The encryption processing apparatus according to Claim 1, wherein said encryption processing apparatus has a memory for storing processing results of the encryption processing units which form the mixed encryption processing sequence set by said control section, and

said control section is configured to store the processing results in said memory to identify which encryption processing unit the processing results are obtained from.

Claim 9 (Previously Presented): An encryption processing apparatus configured to perform a data encryption process, said encryption processing apparatus comprising:

a processor configured to provide:

a control section configured to set a mixed encryption processing sequence by dividing an original encryption processing sequence into a plurality of groups, each group being composed of a plurality of encryption processing units, each encryption processing unit being a defined process, each group being a separate and independent encryption process for encrypting an input data, where a first input data to be encrypted for a first group of the groups is different relative to a second input data to be encrypted for a second one of the groups and the first input data to be encrypted for the first group is generated independently relative to the second input data to be encrypted for the second group, said control section adding dummy encryption processing units as encryption processing units to at least one of the groups that performs dummy encryption processes that are unnecessary for the original encryption processing sequence, and said control section performing a mixing of processing sequences of the encryption processing units of the plurality of groups with each other by executing performance of at least one encryption processing unit from the first group at a time between executing performance of encryption processing units from the second group;

an encryption processing section configured to perform an encryption process in accordance with the mixed encryption processing sequence set by said control section; and

a transmitting unit configured to transmit each of encrypted output data generated independently by the first group and the second group to an external device.

Claim 10 (Previously Presented): The encryption processing apparatus according to Claim 9, wherein an encryption processing unit contained in said original encryption processing sequence is a single-DES encryption process,

said control section is configured to set said dummy encryption processes as single-DES encryption processes and

wherein said control section is configured to set the number of dummy encryption processes to a multiple of 3.

Claim 11 (Previously Presented): An encryption processing method, implemented on an encryption processing apparatus, for performing a data encryption process, said encryption processing method comprising:

dividing, at the encryption processing apparatus, an original encryption processing sequence into a plurality of groups, each group being composed of a plurality of encryption processing units, each encryption processing unit being a defined process, each group being a separate and independent encryption process for encrypting an input data, where a first input data to be encrypted for a first group of the groups is different relative to a second input data to be encrypted for a second group of the groups, and the first input data to be encrypted for the first group is generated independently relative to the second input data to be encrypted for the second group;

setting, at the encryption processing apparatus, a mixed encryption processing sequence by mixing processing sequences of encryption processing units of the plurality of groups with each other by executing performance of at least one encryption processing unit from the first group at a time between executing performance of encryption processing units from another the second group and under a condition in which a processing sequence of the encryption processing units, set in said dividing, within each group is fixed; and

performing, at the encryption processing apparatus, an encryption process in accordance with the mixed encryption processing sequence set in said setting; and

transmitting, from the encryption processing apparatus, each of encrypted output data generated independently by the first group and the second group to an external device.

Claim 12 (Previously Presented): The encryption processing method according to Claim 11, wherein each group includes a triple-DES encryption process and said dividing includes setting a dummy single-DES process as a dummy encryption process that is unnecessary for the original encryption processing sequence in at least one of said groups, and setting the number of single-DES processes of dummies to be set to a multiple of 3, said method further comprising:

setting a dummy encryption processing unit that performs the dummy encryption process in at least one of the groups, and

setting the mixed encryption processing sequence by mixing the encryption processing units of a plurality of groups containing said dummy encryption processing unit ~~units~~.

Claim 13 (Previously Presented): The encryption processing method according to Claim 11, wherein said dividing determines a group of sequences, which can be performed independently of each other, within the original encryption processing sequence to be divided in a process of division into the plurality of groups, and performs a process for setting a group of divisions in which each of the sequences in the group of sequences can be performed independently as a unit.

Claim 14 (Previously Presented): The encryption processing method according to Claim 11, wherein each of said encryption processing units is a single-DES encryption process,

said dividing divides the original encryption processing sequence containing one or more single-DES encryption processes into a plurality of groups composed of one or more single-DES encryption processes, and

said setting sets one mixed encryption processing sequence by mixing the single-DES encryption processing units contained in each group by mutual replacement of the single-DES encryption processing units of each set group under the condition in which the processing sequence within each set group is fixed.

Claim 15 (Previously Presented): The encryption processing method according to Claim 11, wherein

said dividing performs a process for dividing the encryption processing sequence into a plurality of groups composed of one or more encryption processing units with a single-DES encryption process which forms a triple-DES encryption process being an encryption processing unit.

Claim 16 (Previously Presented): The encryption processing method according to Claim 11, wherein the original encryption processing sequence to be mixed is an encryption processing sequence including a random-number generation process, and

said encryption processing method further comprises forming a random-number generation process as a process including a conversion process by three single-DES processes and setting the three single-DES processes as a random-number generation process in one of the groups.

Claim 17 (Canceled).

Claim 18 (Previously Presented): The encryption processing method according to Claim 11, further comprising:

storing processing results in a memory for storing processing results of the encryption processing units which form the mixed encryption processing sequence to identify which encryption processing unit the processing results are obtained from.

Claim 19 (Previously Presented): An encryption processing method, implemented on an encryption processing apparatus, for performing a data encryption process, said encryption processing method comprising:

dividing, at the encryption processing apparatus, an original encryption processing sequence, into a plurality of groups, each group being composed of a plurality of encryption processing units, each encryption processing unit being a defined process, each group being a separate and independent encryption process for encrypting an input data, where a first input data to be encrypted for a first group of the groups is different relative to a second input data to be encrypted for a second group of the groups, and the first input data to be encrypted for the first group is generated independently relative to the second input data to be encrypted for the second group,

setting, at the encryption processing apparatus, a mixed encryption processing sequence by adding dummy encryption processing units as encryption processing units to at least one of the groups, the dummy encryption processing units performing dummy encryption processes that are unnecessary for the original processing sequence and by mixing processing sequences of the encryption processing units of the plurality of groups with each other by executing performance of at least one encryption processing unit from the first group at a time between executing performance of encryption processing units from the second group;

performing, at the encryption processing apparatus, an encryption process in accordance with said mixed encryption processing sequence; and

transmitting, from the encryption processing apparatus, each of encrypted output data generated independently by the first group and the second group to an external device.

Claim 20 (Previously Presented): The encryption processing method according to Claim 19, wherein an encryption processing unit contained in said original encryption processing sequence is a single-DES encryption process,

said setting sets said dummy encryption processes as a single-DES encryption process, and

wherein said dividing includes setting the number of dummy encryption processes to a multiple of 3.

Claim 21 (Previously Presented): A non-transitory computer readable storage medium encoded with computer executable instructions, which when executed by a computer, cause the computer to perform a method comprising:

dividing an original encryption processing sequence into a plurality of groups, each group being composed of a plurality of encryption processing units, each encryption processing unit being a defined process, each group being a separate and independent encryption process for encrypting an input data, where a first input data to be encrypted for a first group of the groups is different relative to a second input data to be encrypted for a second group of the groups, and the first input data to be encrypted for the first group is generated independently relative to the second input data to be encrypted for the second group;

setting a mixed encryption processing sequence by mixing processing sequences of encryption processing units of the plurality of groups with each other by executing performance of at least one encryption processing unit from the first group at a time between

executing performance of encryption processing units from the second group and under a condition in which a processing sequence of the encryption processing units, set in said dividing, within each group is fixed;

performing an encryption process in accordance with the mixed encryption processing sequence set in said setting; and

transmitting each of encrypted output data generated independently by the first group and the second group to an external device.

Claim 22 (Previously Presented): A non-transitory computer readable storage medium encoded with computer executable instructions, which when executed by a computer, cause the computer to perform a method comprising:

dividing an original encryption processing sequence, into a plurality of groups which each include a plurality of encryption processing units, each encryption processing unit being a defined process, each group being a separate and independent encryption process for encrypting an input data, where a first input data to be encrypted for a first group of the groups is different relative to a second input data to be encrypted for a second group of the groups, and the first input data to be encrypted for the first group is generated independently relative to the second input data to be encrypted for the second group;

setting a mixed encryption processing sequence by adding dummy encryption processing units as encryption processing units to at least one of the groups, the dummy encryption processing units performing dummy encryption processes that are unnecessary for the original processing sequence and by mixing processing sequences of the encryption processing units of the plurality of groups with each other by executing performance of at least one encryption processing unit from the first group at a time between executing performance of encryption processing units from the second group; and

performing an encryption process in accordance with said mixed encryption processing sequence; and

transmitting each of encrypted output data generated independently by the first group and the second group to an external device.

Claim 23 (New): The encryption processing apparatus according to Claim 1, wherein the first input data to be encrypted for the first group is received from the external device, the second input data to be encrypted for the second group is a random number generated at the encryption processing apparatus, and each of encrypted output data generated independently by the first group and the second group that is sent to the external device is used to verify that the encryption processing apparatus and the external device share a valid common key.